UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/815,396	03/31/2004	Christopher J. Lord	110466-152116	7579

31817 7590 04/01/2009

SCHWABE, WILLIAMSON & WYATT, P.C.
PACWEST CENTER, SUITE 1900
1211 S.W. FIFTH AVE.
PORTLAND, OR 97204

EXAMINER	
ZHANG, SHIRLEY X	

ART UNIT	PAPER NUMBER
2444	

MAIL DATE	DELIVERY MODE
04/01/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/815,396	LORD ET AL.	
	Examiner	Art Unit	
	SHIRLEY X. ZHANG	2444	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 December 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9,11-14,16-32,34 and 35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9,11-14,16-32,34 and 35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This final office action is prepared in response to the applicant's amendments and arguments filed on December 17, 2008 as a reply to the non-final office action mailed on August 18, 2008.

No claim has been amended;

Claims 1-9, 11-14, 16-32 and 34-35 are now pending;

Response to Arguments

Applicant's arguments and amendments filed on December 17, 2008 have been carefully considered but deemed unpersuasive for reasons provided by the examiner below.

Accordingly, THIS ACTION IS MADE FINAL. See MPEP 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

1. Rejections to claims 1 and 27 under 35 U.S.C. 112, first paragraph are maintained. See the section "***Claim Rejections - 35 USC § 112***" below for the examiner's explanation.

2. Rejections to claims 1-9, 11-14, 16-32 and 34-35 under 35 U.S.C. 112, first paragraph are maintained.

Regarding claim 1, Applicant argued that "Nothing in Cho teaches or suggests that the control point may move outside the home network." (Arguments/Remarks, page 11, last paragraph).

Examiner respectfully disagrees with the applicant's interpretation of Cho's disclosure in [0005]-[0006] and asserts that

Cho disclosed in [0005] a conventional system for controlling and managing devices in a home network by a user through user interface and UPnP API while they are all present in one system, i.e. one home network.

Cho then disclosed in [0006-0007] that a problem associated with the conventional system disclosed in [0005] is that when the user is beyond the home network, such as beyond the limited range that messages sent within the home network cannot be received, the conventional system is not functional.

Therefore, Cho disclosed that a user may move outside the home network.

Cho further disclosed in Fig. 1 and [0026] that

the invention is about "a proxy system for a home gateway designed to allow a user to control UPnP devices 150 in a home network 140 over an external Internet network using a wired/wireless Internet client 100 or 110," which means that when a user moves outside the home network, it is actually the wireless Internet client 110 carried by the user, i.e. the control point, that moves outside the home network.

Therefore, to the contrary of what Applicant has pointed out, Cho's disclosure in [0005-0006] and [0026], when read as a whole, indeed suggested that the control point (i.e. "wired/wireless Internet client 100 and 110" in Fig. 1) may move outside the home network.

Further regarding claim 1, Applicant disagreed with the Examiner's reading of Cho's UPnP proxy server as the intermediary in claim 1. Applicant argued that "none of the figures

disclose that the agent or the bridge of the UPnP proxy in Cho would determine as in claim 1 that if the messages belong to a communication session between the UPnP device on the home network and another device that roamed out from the home network."

In response, Examiner would like to point out that

(1) the proxy server in Cho is equivalent to the intermediary in claim 1 because Cho's proxy server relays control messages between the wired/wireless Internet client outside the home network and the UPnP devices in the home network. Although Cho did not explicitly disclose

(2) claim 1 does not recite "determining if the messages belong to a communication session between the UPnP device on the home network and another device that roamed out from the home network" as presented in the argument quoted above.

(3) Cho disclosed that the control point represented by a wired/wireless Internet client may move outside a home network, implying that messages sent by the control point while it is moving outside the home network may be received by the proxy server if the control point successfully attach to the Internet. The proxy server may generate an error message, as generating an error message in response to messages no longer considered valid is a common knowledge well within one of ordinary skill in the art of computer/communications network.

Further regarding claim 1, Applicant argues that there would have been no motivation to modify Cho to achieve what is recited in claim 1.

However, Examiner respectfully disagrees. Both Cho and Moyer disclosed controlling devices in a home network over external Internet (Cho, Fig. 1 and [0012], "managing and controlling UPnP devices in a home network over an external Internet network"; Moyer, Fig. 1

and [0012], "allow control of a device in the home from the outside world"). Moyer further disclosed the need to address the problem of wide area access and security in prior systems, of which Cho's system is one example.

Therefore, Moyer's disclosure of the need for security and means for providing security would have motivated one of ordinary skill in the art to modify Cho to adopt Moyer's security measures.

Applicant's arguments regarding claims 23, 27, 12, 8, 21 and 26 are similarly addressed.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claims 1 and 27 are rejected under 35 U.S.C. 112, first paragraph, as based on a disclosure which is not enabling. Critical or essential to the practice of the invention, but not included in the claim(s) is not enabled by the disclosure. See *In re Mayhew*, 527 F.2d 1229, 188 USPQ 356 (CCPA 1976).

The claim recites the following element that is critical or essential to the practice of the invention

"receiving network traffic from the second device corresponding to a previous secure communication session established when the second device was previously on the internal

network; and responding to said network traffic with an error such that the second device attempts to re-establish a secure communication session from the external network."

However, the above claim element is not enabled by the disclosure in either the claim or the specification because it is unclear how "receiving network traffic from the second device corresponding to a previous secure communication session" can take place when the second device moves to the external network while still using the IP address that belongs to the internal network.

When the second device is in the internal network, traffic from the second device corresponding to a secure session is sent directly to the first devices without going through the intermediary. When the second device moves outside the internal network, traffic from the second device corresponding to the said secure session will be addressed to the first device directly.

In response to Examiner's reason for rejection presented in the previous office action, Applicant stated on page 10 of the "Arguments/Amendments" filed on December 19, 2008 that

"a mobile control point (which may be deemed as the second device) having a previously established secured communication session with a device (which may be deemed as the first device) on the internal network may have a new attachment to the external network. The traffic of this previously established communication session will route to the gateway of the internal network, and the gateway would force the control point to reestablish a communication session."

Examiner understands the applicant's statement of "may have a new attachment to the external network."

However, Examiner considers the process of establishing a new attachment to the external network an essential element of the claimed invention, but not sufficiently disclosed in the specification to enable one of ordinary skill in the art to reproduce the process of establishing a new attachment without undue experimentation.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. **Claims 1-7, 9, 11, 23-25, 27-31** are rejected under 35 U.S.C. 103(a) as being unpatentable over Cho et al. (U.S. PG-Pub No. 2003/0217136, hereinafter "**Cho**"), in view of Moyer et al. (U.S. PG-Pub No. 2002/0103898, hereinafter "**Moyer**").

Regarding claim 1, Cho disclosed a method for an intermediary selectively coupling an external network and an internal network to dynamically generate filter rules to facilitate establishing an end to end session connection between a first device on the internal network and a second device of the external network (Fig. 1 and [0026] disclose the proxy server 130 that is equivalent to the intermediary recited in the claim), the method comprising:

receiving a session establishment request by the second device on the external network to establish a communication session with the first device on the internal network (Fig.7 and [0026] disclose that the UPnP proxy server includes an agent 131 for receiving a command from the wired and wireless clients 100 or 110 on the Internet);

forwarding the session establishment request to the first device (Fig.7 and [0026] disclose that the UPnP proxy server also includes a bridge for sending control messages to the UPnP devices in the home network);

monitoring the internal network for an approval or disapproval acknowledgement by the first device for the session establishment request (Fig.2, Fig.7 and [0026] disclose that the bridge receive event messages from the UPnP devices, where the event messages include responses to the previously sent control messages); and

receiving network traffic from the second device corresponding to a previous secure communication session established when the second device was previously on the internal network and responding to said network traffic with an error such that the second device attempts to re-establish a secure communication session from the external network ((Cho, [0005-0006] disclosed that in a conventional UPnP network, a control point receives advertisement messages while in the home network; Cho, [0006] further disclosed that the control point may travel outside the home network, and that the control point may be a wireless client as shown in Fig. 1; Such disclosure means that a control point may still be sending traffic belonging to a previous session to the home network as it travels beyond the range of the home network, causing an error condition to be generated).

Cho did not explicitly disclose the session establishment request is a secure session request. Neither did Cho explicitly disclosed configuring a first filter rule of the intermediary to allow communication between the first and second devices through the intermediary, if an approval acknowledgement is detected;

However, Moyer disclosed a method for remotely controlling home appliances in a home network from outside network such as Internet using a Home Firewall/NAT (RGW) that authenticates and authorizes each request/message from external sources so as to filter and reject communications from unknown sources for security reasons (Moyer, [0072], [0078-0080]). The disclosure implies that the firewall must be configured filter rules, and the session between a control source and a networked appliance is secure.

One of ordinary skill in the art would have been motivated to combine Cho and Moyer because both disclosed controlling devices in a home network over external Internet (Cho, Fig. 1 and Moyer, Fig. 1).

Therefore, it would have been obvious for one to incorporate Moyer's security features such as Firewall/NAT into Cho to achieve the desirable result of securing the communications between Cho's wired/wireless internet client and UPnP home devices so that the UPnP devices will not be tempered by malicious clients from the internet.

Claim 27 lists substantially the same elements of **claim 1**, but in product form rather than method form. Therefore, the supporting rationale of the rejection to **claim 1** applies equally as well to **claim 27**.

Regarding claims 2 and 28, the combination of Cho and Moyer disclosed the method of claim 1, and the article of claim 27, respectively.

Cho further disclosed that the method comprises:

determining a presence advertisement for the first device has been received before forwarding the secure session establishment request to the first device (Cho, Fig. 2, Fig. 7 and [0039] disclose that the device management module 21 is adapted to receive advertisement messages periodically sent from the UPnP devices in the home network, manage a device list on the basis of the received advertisement messages and, when a new UPnP device is additionally provided in the home network, receive a device description from the new UPnP device).

Regarding claim 3, the combination of Cho and Moyer disclosed the method of claim 2.

Cho further disclosed that the presence advertisement is delivered in accordance with the UPnP Simple Service Discovery Protocol (SSDP) (Cho, [0008] discloses using SSDP, a protocol proposed to be used in UPnP network for presence advertisement).

Regarding claim 4, the combination of Cho and Moyer disclosed the method of claim 1. Cho further disclosed that the method comprises:

receiving network traffic from the second device corresponding to the second device requesting a UPnP Device Description Document from the first device (Cho, Fig. 7 and [0071] disclose that upon receiving a service description request message from the stub 102 (step 717), the agent 131 sends the received message to the bridge 132 (step 718), which then transfers it to the specific UPnP device (step 719)).

Regarding claims 5, 29, the combination of Cho and Moyer disclosed the method of claim 1, the article of claim 27, respectively.

Cho further disclosed:

receiving a service request from the second device for the first device, the service request having an associated communication port for performing the service (Cho, Fig. 7, "device control command 729"; Cho, [0044] further disclosed that the message processing module on the UPnP Proxy conducts communications according to HTTP protocol; As HTTP is a TCP based protocol, a service request such as the "device control command" inherently has an associated communication port);

determining the service request identifies a service advertised by the first device in a device description document (Cho, Fig. 7 and [0040]); and

configuring a second filter rule to allow communication between the first device and the second device using the associated communication port (Cho, [0007] disclosed that a home network can be a private network and [0008] disclosed using NAT; For NAT, a filter rule must exist in the proxy device to translate between the public IP address and private IP address to allow communication between home network and Internet).

Regarding claims 6 and 30, the combination of Cho and Moyer disclosed the method of claim 1 and the article of claim 27 respectively.

Cho further disclosed that the method comprises:

providing the second device with an indicia for use by the second device in establishing a communication link to the first device (Fig.7 and [0071] disclose that the specific UPnP device sends the service description to the bridge 132 (720), which then transfers it to the agent 131 (721), where the service description is equivalent to the indicia recited in the claim).

Regarding claim 7, the combination of Cho and Moyer disclosed the method of claim 1.

Cho further disclosed that the indicia is a selected one of a globally routable Internet Protocol (IP) address, or an internal network address non-routable on the external network (Cho, [0008] discloses a method that is adapted to control UPnP devices with private Internet protocol (IP) addresses in a home network over the Internet by providing on the Internet a UPnP directory server that translates uniform resource locator (URL) information in device descriptions of the UPnP devices by way of a network address translation (NAT) technology and provides the translated information to a client on an external Internet network; as NAT translates between public and private IP addresses, IPv6 and IPv4 address, or private IP addresses of different subnets, the use of NAT in Le implies that the address returned to the UE in the external network is either a public IP address, or a private IP address).

Regarding claims 9 and 31, the combination of Cho and Moyer disclosed the method of claim 1 and the article of claim 27, respectively.

Cho did not explicitly disclose retrieving an Access Control List (ACL) from the first device, the ACL including an identification of devices authorized to establish communication sessions; and determining based at least in part on the ACL the second device is authorized to establish the secure communication session with the first device before forwarding the secure session establishment request to the first device.

However, Moyer disclosed that a SIP UAS device is responsible for authenticating the originator of the message, and determine if that originator is authorized to perform the requested

operation by consulting an access control list (Moyer, [0020]). Moyer further disclosed that the Home UAS (i.e. Firewall/NAT in Fig. 3) must filter and reject communications from unknown sources (Moyer, [0078]).

Examiner provides the same rationale for combining Cho and Moyer as provided above in the rejection of claim 1.

Regarding claim 11, the combination of Cho and Moyer disclosed the method of claim 1.

Cho did not explicitly disclosed but Moyer disclosed establishing the end to end secure session connection between the first device on the internal network and the second device of the external network in a single end to end secure session connection between said first and second devices (Moyer, [0022] disclosed that messages between the client control application and a networked appliance is grouped into a session through authentication tools and security mechanisms, making the session secure).

Examiner provides the same rationale for combining Cho and Moyer as provided above in the rejection of claim 1.

Regarding claim 23, Cho disclosed a system of devices communicatively coupled with an internal network and an external network via a gateway (Cho, Fig. 1, UPnP Proxy server), comprising:

a first device, communicatively coupled to the internal network, offering services (Cho, Fig.1, UPnP devices); a second device selectively coupled with the internal and external networks,

the second device seeking a service of the first device (Cho, Fig.1, wired/wireless internet clients),

wherein when requesting the service, said requesting includes sending a communication initiation request to the first device to facilitate establishing a communication session with the first device; and an intermediary selectively communicatively coupling the first and second devices, wherein the intermediary is configured to receive a communication initiation request from the second device over the external network and forward the request to the first device (Cho, Fig. 1 discloses the wired/wireless internet clients sending control messages to the UPnP device via the UPnP Proxy server as an intermediary, which forwards messages to the UPnP device).

Cho did not explicitly disclose that the session to be established is a secure session.

However, Moyer disclosed a method for remotely controlling home appliances in a home network from outside network such as Internet via a Home Firewall/NAT (RGW) which authenticates and authorizes each request/message from external sources so as to filter and reject communications from unknown sources for security reasons, (Moyer, [0072], [0078-0080]), making the session between a control source and a networked appliance secure.

One of ordinary skill in the art would have been motivated to combine Cho and Moyer because both disclosed controlling devices in a home network over external Internet (Cho, Fig. 1 and Moyer, Fig. 1).

Therefore, it would have been obvious for one to incorporate Moyer's security features such as Firewall/NAT into Cho to achieve the desirable result of securing the communications between Cho's wired/wireless internet client and UPnP home devices so that the UPnP devices will not be tempered by malicious clients from the internet.

Regarding claim 24, the combination of Cho and Moyer disclosed the system of claim 23.

Cho did not explicitly disclose but Moyer disclosed that the intermediary is further configured to monitor the first device for an approval or disapproval authentication acknowledgement for the request, and to configure a filter of the intermediary controlling communication over the first network from the first device based at least in part on a monitored authentication acknowledgement.

However, Moyer disclosed a method for remotely controlling home appliances in a home network from outside network such as Internet using a Home Firewall/NAT (RGW). Moe specifically, Moyer disclosed in [0020], [0023] and [0079] that the firewall authenticates the originator of a message, and then determine if the originator is authorized to perform the requested operation, meaning that if the originator is not authorized, the request message will be blockedExaminer provides the same rationale as provided in claim 23 for the combination of Cho and Moyer.

Examiner provides the same rationale as provided in claim 23 for the combination of Cho and Moyer.

Regarding claim 25, the combination of Cho and Moyer disclosed the system of claim 23.

Cho further disclosed that the first device communicates with the second device in accord with the UPnP Security Protocol (Cho, Fig. 1).

5. **Claims 12-14, 16-20, 22, 32 and 34-35** are rejected under 35 U.S.C. 103(a) as being unpatentable over Cho et al. (U.S. PG-Pub No. 2003/0217136, hereinafter "**Cho**"), IETF draft "Simple Service Discovery Protocol/1.0" (hereinafter "**IETF-Draft-SSDP**"), and Moyer et al. (U.S. PG-Pub No. 2002/0103898, hereinafter "Moyer").

Regarding claim 12, Cho disclosed a method for a second device communicating with a first device on an internal network by way of an intermediary selectively coupling an external network and the internal network (Cho, Fig. 1 and [0026] disclose the proxy server 130 coupling internet and a home network), comprising:

receiving, by the second device while on the internal network, a presence advertisement for the first device (Cho, Fig. 2, Fi.g7 and [0039] disclosed that the device management module 21 is adapted to receive advertisement messages periodically sent from the UPnP devices in the home network, manage a device list on the basis of the received advertisement messages and, when a new UPnP device is additionally provided in the home network, receive a device description from the new UPnP device);

storing, by the second device while on the internal network, a network address associated with the first device (Cho, [0015] discloses a method of allowing the UPnP proxy server to

discover the UPnP devices in the home network, acquire information of the UPnP devices, create a device list on the basis of the acquired information; Cho, [0008] further discloses that a UPnP SSDP protocol is used, as SSDP was proposed by Microsoft as the protocol of choice for device discovery, see "IETF-Draft-SSCP-01"; furthermore, the SSDP draft discloses in section 5.2.1.1 an example of the presence announcement message, which includes a network address associated with the UPnP device; therefore, it can be implied that the UPnP proxy server stores a network address of the device in the device list).

determining, by the second device while on the internal network, services offered by the device (IETF-Draft-SSCP, section 5.2.1.1 discloses that the presence announcement messages contains a value "NT" which indicates the type of service offered by the device); and

Issuing, by the second device while on the external network, a communication initiation request to the first device via the intermediary (Cho, Fig.7 disclose that the UPnP client sends commands to the UPnP device via the UPnP Proxy).

Cho did not explicitly disclosed that the request for the initiation of a secure communication session.

However, Moyer disclosed a method for remotely controlling home appliances in a home network from outside network such as Internet via a Home Firewall/NAT (RGW) which authenticates and authorizes each request/message from external sources so as to filter and reject communications from unknown sources for security reasons, (Moyer, [0072], [0078-0080]), making the session between a control source and a networked appliance secure.

One of ordinary skill in the art would have been motivated to combine Cho and Moyer because both disclosed controlling devices in a home network over external Internet (Cho, Fig. 1 and Moyer, Fig. 1).

Therefore, it would have been obvious for one to incorporate Moyer's security features such as Firewall/NAT into Cho to achieve the desirable result of securing the communications between Cho's wired/wireless internet client and UPnP home devices so that the UPnP devices will not be tempered by malicious clients from the internet.

Examiner asserts that the steps of receiving a presence advertisement and storing a network address for the first device by the second device while on the internal network is a standard UPnP process for any device in a home network, which process is also disclosed by Cho in paragraph [0007]. Therefore, these steps do not distinguish the claimed invention from prior art.

Examiner further asserts that because the claim does not disclose how the second device utilize information received while on the internal network when it moves to the external network, Applicant's remark that in claim 12 the second device can roam between the home network and external network is anticipated by Cho's wireless push client, as a wireless device is known to be able to roam between networks.

Claim 32 lists substantially the same elements of **claim 12**, but in product form rather than method form. Therefore, the supporting rationale of the rejection to **claim 12** applies equally as well to **claim 32.**

Regarding claim 13, the combination of Cho, IETF-Draft-SSDP, and Moyer disclosed the method of claim 12.

Cho further disclosed that the intermediary is configured to:

forward the request to the first device (Fig.7 and [0026] disclose that the UPnP proxy server also includes a bridge for sending control messages to the UPnP devices in the home network);

monitor for an approval or disapproval authentication acknowledgement to the request (Fig.2, Fig.7 and [0026] disclose that the bridge receive event messages from the UPnP devices, where the event messages include responses to the previously sent control messages); and

Cho did not explicitly disclose configuring a filter of the intermediary to allow communication with the first device if an approval authentication acknowledgement is received.

However, in the same field of endeavor, Moyer disclosed using firewall filter and authenticate requests/messages from an external source (Moyer, [0072], [0078-0080] disclosed a method for remotely controlling home appliances in a home network from outside network such as Internet using a Home Firewall/NAT (RGW) that authenticates and authorizes each request/message from external sources so as to filter and reject communications from unknown sources for security reasons). The disclosure implies that the firewall must be configured filter rules, and the session between a control source and a networked appliance is secure.

Examiner provides the same rationale as provided in claim 12 for the combination of Cho and Moyer.

Regarding claim 14, the combination of Cho, IETF-Draft-SSDP, and Moyer disclosed the method of claim 13.

Cho did not explicitly disclose but Moyer disclosed that the intermediary is further configured to configure the filter to block communication with the device is a disapproval authentication acknowledgement is received (Moyer, [0020], [0023] and [0079] disclosed that the firewall authenticates the originator of a message, and then determine if the originator is authorized to perform the requested operation, meaning that if the originator is not authorized, the request message will be blocked).

Examiner provides the same rationale as provided in the rejection of claim 13 for the combination of Cho and Moyer.

Regarding claims 16 and 34, the combination of Cho, IETF-Draft-SSDP and Moyer disclosed the method of claim 12 and the article of claim 32, respectively.

Cho further disclosed that while on the internal network, the method comprises requesting a description of services offered by the device (Cho, [0006] disclosed that the control point acquires all information necessary for the control of the devices in the home network from advertisement messages sent from the devices; Fig. 7 further disclosed in step 718 that the UPnP Proxy server requests a description of services offered by the device from the bridge interfacing to the internal network).

Regarding claim 17, the combination of Cho, IETF-Draft-SSDP and Moyer disclosed the method of claim 16. Cho further disclosed that the description of services is requested from

the intermediary (Cho, Fig.17 discloses in steps 717 and 723 that the UPnP client requests the description of services from the UPnP proxy server, which is an intermediary).

Regarding claims 18 and 35, the combination of Cho, IETF-Draft-SSDP, and Moyer disclosed the method of claim 12 and the article of claim 32, respectively.

Cho further disclosed that while on the external network, the method further comprising requesting a description of services offered by the device (Cho, Fig.17 discloses in steps 717 that the UPnP client, being on the external network, requests the description of services from the UPnP proxy server).

Regarding claim 19, the combination of Cho, IETF-Draft-SSDP, and Moyer disclosed the method of claim 18.

Cho further disclosed that the description of services is requested from the intermediary (Cho, Fig.17 discloses in steps 717 that the UPnP client requests the description of services from the UPnP proxy server, which is an intermediary).

Regarding claim 20, the combination of Cho, IETF-Draft-SSDP, and Moyer disclosed the method of claim 12.

Cho did not disclose but Moyer disclosed receiving an approval authentication acknowledgement to the request; and responsive to the approval, requesting a service of the device (Moyer, [0020], [0023] and [0072]);

Examiner provides the same rationale as provided in claim 12 for the combination of Cho and Moyer.

Regarding claim 22, the combination of Cho, IETF-Draft-SSDP, and Moyer disclosed the method of claim 12.

Cho further disclosed that a traveling control point performs the method for communicating with the device (Cho, Fig.1 discloses that a wireless internet client 110 communicates with the UPnP devices in a home network).

6. **Claim 8** is rejected under 35 U.S.C. 103(a) as being unpatentable over Cho and Moyer as applied to claim 1 above, further in view of Le et al. (U.S. PG-Pub No. 2005/0111382, hereinafter "**Le**").

Regarding claim 8, the combination of Cho and Moyer disclosed the method of claim 1.

Cho did not explicitly disclose but Le disclosed that communication within the internal network is in accord with an IPv6 compatible Internet Protocol (IP) (Le, [0014] discloses that the architecture as illustrated in FIG. 1 has been recently adopted in 3GPP for the internetworking of IPv6 and IPv4 domains; In 3GPP, it is inherent that the internal network uses IPv6).

It would have been obviousness for one of ordinary skill to combine Cho and Le such that a firewall is employed to allow communications between authenticated sessions only by using dynamically configured filtering rules.

One would have been motivated to combine as such by Le's teaching of using an Internet firewall to secure an internal network from the Internet to the extent that it blocks unsolicited traffic from the outside.

7. **Claim 21 is** rejected under 35 U.S.C. 103(a) as being unpatentable over Cho, IETF-Draft-SSDP, and Moyer as applied to claim 12 above, further in view of IETF RFC 3056, "Connection of IPv6 domains via IPv4 clouds", hereinafter "**RFC 3056**".

Regarding claim 21, the combination of Cho, IETF-Draft-SSDP and Moyer disclosed the method of claim 12.

Cho did not explicitly disclose but RFC 3056 disclosed using the prefix of a globally unique IPv6 address to identify an intermediary that connects an IPv6 cloud to the IPv4 network.

It would have been obvious for one of ordinary skill to combine Cho and RFC 3056 so that the intermediary is identified by an IPv6 address prefix, which is a port of the IPv6 address. One would have been motivated to combine as such by Cho's disclosure of using private network to construct home network due to depletion of IPv4 addresses, which problem can be solved by introducing IPv6 into the home network and keeps IPv4 for the external network.

8. **Claim 26** is rejected under 35 U.S.C. 103(a) as being unpatentable over Cho and Moyer as applied to claim 23 above, further in view of the article "UPnP™ Security Ceremonies Design

Document For UPnP Device Architecture 1.0" authored by Ellison and published by the UPnP Forum (hereinafter "**Ellison**").

Regarding claim 26, the combination of Cho and Moyer disclosed the system of claim 23.

Cho did not explicitly disclose but Ellison disclosed that the secure communication initiation request corresponds to a UPnP Set Session Key (SSK) request (Ellison, page 13, section 5, "Session Keys").

It would have been obvious for one of ordinary skill in the art to combine Cho and Ellison so that the secure communication initiation request corresponds to a UPnP set session key request. One would have been motivated to combine Cho and Ellison by Ellison in that Ellison first discloses the need in UPnP for a security protocol and then suggested using Session Key to establish end-to-end secure sessions.

Conclusion

THIS ACTION IS FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR

1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SHIRLEY X. ZHANG whose telephone number is (571)270-5012. The examiner can normally be reached on Monday through Friday 8:00am - 5:30pm EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Vaughn can be reached on (571) 272-3922. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Shirley X. Zhang/
Examiner, Art Unit 2444
3/20/2009

/William C. Vaughn, Jr./

Supervisory Patent Examiner, Art Unit 2444